FY 2005 ITL Publications

Note that some documents are published in more than one place. Due to the large number of documents, publications listed in previous ITL Technical Accomplishment reports are not repeated.

Author	Title	Place of Publication	Date
Avilés, A.I., Ankenman, B.E., Pinheiro, J.C.	Assembled Designs for Estimation of Location, Dispersion, and Random Effects	Technometrics	

In many experimental settings, different types of factors affect the measured response. The factors that can be set independently of each other are called crossed factors. Nested factors cannot be set independently because the level of one factor takes on a different meaning when other factors are changed. Random nested factors arise from quantity designations and from sampling and measurement procedures. The variances of the random effects associated with nested factors are called variance components. Factor effects on the average are called location effects. Dispersion effects are the effects of the crossed factors on the variance of a response. For situations where crossed factors have effects on the different variance components, then sets of dispersion effects must be identified and estimated to achieve robustness. The main objective of this research is to provide nearly D-optimal experimental design procedures for estimating the location effects of crossed factors, the variance components associated with two nested factors, and the dispersion effects that crossed factors may have on the two variance components. A general class of experimental designs for mixed-effects models with random nested factors, called assembled designs, is introduced in Ankenman, Avilés, and Pinheiro (2003). The use of assembled designs for robustness experiments is introduced. When there are dispersion effects, a heuristic algorithm for finding a nearly D-optimal assembled design with two variance components for a given budget is provided. Ready to use computer programs for the presented experimental design procedures and analysis technique are discussed. This research provides the practitioner with clear guidelines about the best design available for their needs.

Beichl, I., Bullock, S., Song, D.	A Quantum Algorithm Detecting Concentrated Maps	NIST Journal of Research	

Let for , some number of quantum bits. Using calls to a classical oracle evaluating and an -bit memory, it is possible to determine whether is one-to-one. For some radian angle , we say is -concentrated iff for some given and any . This manuscript presents a quantum algorithm that distinguishes a -concentrated from a one-to-one in calls to a quantum oracle function with high probability. For radians, the quantum algorithm outperforms the obvious classical algorithm on average, with maximal outperformance at radians. Thus, the constructions generalize Deutsch's algorithm, in that quantum outperformance is robust for (slightly) nonconstant .

Author	Title	Place of Publication	Date
Bowdrey, M.D., Jones, J.A., Knill, E., Laflamme, R.	Compiling Gate Networks on an Ising Quantum Computer	http://arxiv.org/quant-ph and Physical Review A	

Here we describe a simple mechanical procedure for compiling a quantum gate network into the natural gates (pulses and delays) for an Ising quantum computer.

Bullock, S.S., O'Leary, D.P., Brennen, G.K.	Asymptotically Optimal Quantum Circuits for d-level Systems	Physical Review Letters and http://www.arxiv.org/	

As a qubit is a two-level system whose state space is spanned by and , so a qudit is a -level system whose state space is spanned by ,…, . Quantum computation has stimulated much recent interest in algorithms factoring unitary evolutions of an -qubit state space into component two-particle unitary evolutions. In the absence of symmetry, Shende, Markov, and Bullock use Sard's theorem to prove that at least two-qubit unitary evolutions are required, while Vartiainen, Moettoenen, and Salomaa (VMS) use the matrix factorization and Gray codes in an optimal order construction involving two-particle evolutions. In this work, we note that Sard's theorem demands two-qudit unitary evolutions to construct a generic (symmetry-less) -qudit evolution. However, the VMS result applied to virtual qubits only recovers optimal order in the case that is a power of two. We further construct a decomposition for multi-level quantum logics, proving a sharp asymptotic of two-qudit gates and thus closing the complexity question for all –level systems (finite). Gray codes are not required.

Cowley, P., Nowell, L., Scholtz, J.	Glass Box: An Instrumented Infrastructure for Supporting Human Interaction with Information	CD-ROM	10/27/2004

In this paper, we discuss the challenges involved in developing an infrastructure to support a new generation of analytic tools for information analysts. The infrastructure provides data for establishing context about what the analyst is doing with the analytic tools, supports an integration environment to allow suites of tools to work together, and supports evaluation of the analytic tools. We discuss the functionality of the Glass Box, the challenges of evaluating adaptive systems including the capture of data for evaluation metrics, and lessons learned from our experiences to date.

Author	Title	Place of Publication	Date
Dabrowski, C., Mills, K.L., Quirolgico, S.	A Model-Based Analysis of First-Generation Service Discovery	NIST SP 500-260	

Future commercial software systems will be based on distributed service-oriented architectures in which applications are composed dynamically from remote components. A key part of service-oriented computing is the ability for clients to discover remote services that fulfill specific requirements. Since the mid-1990s, various commercial and public domain designs for service discovery systems have been proposed that enable clients and services to rendezvous in a distributed system. The report characterizes such designs as first-generation service discovery systems, based on the belief that experience with these systems will lead to future, improved designs.

Using three widely used service discovery systems as a basis, this publication first presents a high level overview of the operation of service discovery protocols. A detailed generic model of first-generation service discovery systems, written in UML, follows this. The UML model provides an in-depth analysis of the alternative service discovery designs available today, including the major functional components that comprise these designs, the behaviors of these components, and the information they exchange. The report verifies the generality of the model by mapping its component element to corresponding elements of existent and emerging service discovery systems. This report also identifies issues that designers should attempt to resolve in the next generation of service discovery systems.

The analysis is then extended to provide designers of future service discovery systems with a means to evaluate designs. First, the report proposes a set of service goals that service discovery systems should strive to satisfy to ensure a desirable level of quality of service. These goals provide a basis to define metrics, for evaluation the behavior and measuring performance of system designs and implementations. Second, the report identifies potential performance issues that may arise during operation of service discovery systems. Identifying performance issues can alert designers and implementers to the potential for unexpected behavior when service discovery technology is deployed at large scale. The report presents possible solutions to performance problems that extend well-known optimization algorithms for distributed systems and present new algorithms tailored to service discovery environments. The contributions in this report will help to improve the quality of the next generation of service discovery systems on which the service-oriented architectures of tomorrow appear likely to depend. Further, should an industry standards group choose to develop a unified specification for service discovery, the model should provide helpful input to the process.

Davis, R.A., Dunsmuir, W.T.M., Streett, S.B.	Maximum Likelihood Estimation for an Observation Driven Model for Poisson Counts	Methodology and Computing in Applied Probability	

This paper is concerned with an observation driven model for time series of counts whose conditional distribution given past observations follows a Poisson distribution. This class of models is capable of modeling a wide range of dependence structures and is readily estimated using an approximation to the likelihood function. Recursive formulae for carrying out maximum likelihood estimation are provided and the technical components required for establishing a central limit theorem of the maximum likelihood estimates are given in a special case.

Author	Title	Place of Publication	Date
Gallagher, L.J., Offutt, A.J., Cincotta, A.V.	Integration Testing of Object-Oriented Components Using Finite State Machines	Software Testing, Verification, and Reliability (STVR)	

In object-oriented terms, one of the goals of integration testing is to ensure that messages from objects in one class or component are sent and received in the proper order and have the intended effect on the state of external objects that receive the messages. This research extends an existing single-class testing technique to integration testing of multiple classes. The previous method models the behavior of a single class as a finite state machine, transforms that representation into a data flow graph that explicitly identifies the definitions and uses of each state variable of the class, and then applies conventional data flow testing to produce test case specifications that can be used to test the class. This paper extends those ideas to inter-class testing by developing flow graphs and tests for an arbitrary number of classes and components. It introduces flexible representations for message sending and receiving among objects and allows concurrency among any or all classes and components. Data flow graphs are stored in a relational database, and database queries are used to gather def-use information. This approach is conceptually simple, mathematically precise, quite powerful, and general enough to be used for traditional data flow analysis. This testing approach relies on finite state machines, database modeling and processing techniques, and algorithms for analysis and traversal of directed graphs. The paper presents empirical results of the approach applied to an automotive system.

Harman, D.	The History of IDF and its Influences on IR and Other Fields	Chapter in “Progress in Natural Language Processing & Information Retrieval: A Festschrift for Karen Sparck Jones”	

The surprisingly simple IDF measure developed in 1972 by Karen Sparck Jones has continued to dominate the term weighting metrics used in information retrieval, despite several efforts to develop more complex measures of term distribution. It has been incorporated in (probably) all information retrieval systems and used in languages other than English. This chapter presents the origins of the IDF measure and how it evolved into the measure that is used today.

Harman, D.	Text Retrieval Conference and Message Understanding Conference	Encyclopedia of Language and Linguistics	

The Text Retrieval Conferences (TRECs) and the Message Understanding Conferences (MUCs) are two critical evaluation efforts in natural language understanding that in large part have shaped the research in those areas during the 1990s. The TREC work concentrated on research in information retrieval, starting with the basic retrieval task of finding documents in response to a question, but then branching into multiple variations on this central theme. The MUC tests have targeted information extraction, in particular how to find and aggregate specific information on entities such as persons, locations, and organizations, and the relationships between such entities.

Author	Title	Place of Publication	Date
Harman, D.	The Importance of Focused Evaluations: A Case Study of TREC	Chapter in “Progress in Natural Language Processing & Information Retrieval: A Festschrift for Karen Sparck Jones”	

Evaluation has always been an important part of scientific research, and in information retrieval, this evaluation has mostly been done using test collections. In 1992, a new test collection was built at the National Institute of Standards and Technology (NIST), and a focused evaluation (the Text REtrieval Conference or TREC) was started to use the collection. Results from nearly 12 years of this focused evaluation show significant technology transfer across systems, leading to major improvements in system performance. Focused evaluations also create the ability to target specific problems in language technology, such as retrieval across languages, and to design tasks for evaluation such that issues can be studied concurrently by multiple groups. This chapter will discuss some of the tasks that have been examined in TREC, including critical factors in the design of those evaluations. Additionally a second focused evaluation, the Document Understanding Conference (DUC), which evaluates text summarization, will be discussed.

Harman, D., Voorhees, E.M.	TREC: An Overview	Annual Review of Information Science and Technology, Volume 40	

The Text REtrieval Conference (TREC) is a workshop series designed to build the infrastructure necessary for large-scale evaluation of text retrieval technology. Participants in the workshops (over 100 groups in the latest TREC) have been drawn from the academic, commercial, and government sectors, and have included representatives from more than 20 different countries. These collective efforts have accomplished a great deal: a variety of large test collections have been built for both traditional "ad hoc" retrieval and related tasks such as cross-language retrieval, speech retrieval, and question answering; retrieval effectiveness has approximately doubled; and many commercial retrieval systems now contain technology first developed in TREC. This chapter chronicles the first twelve years of TREC, with extensive references to the experiments that have been done during those years.

Author	Title	Place of Publication	Date
Hornikova, A., Guthrie, W.F.	Troubleshooting Key Comparisons	Proceedings of Joint Statistical Meetings 2004, Toronto, Canada	

Key Comparisons are international inter-laboratory studies used to establish the degree of equivalence between national measurement standards. These studies, carried out by National Measurement Institutes, are time-consuming, but necessary to facilitate international trade. Since the signing of the Mutual Recognition Arrangement (MRA) in 1999, approximately sixty Key Comparisons in a wide range of metrological areas have been completed and have results posted in the Key Comparison Database (KCDB) maintained by the International Bureau of Weights and Measures (BIPM) in France and in the International Comparisons Database (ICDB) maintained by the National Institute of Standards and Technology (NIST) in the U.S. As with many new standardized procedures, however, the translation of the guidelines for the conduct of Key Comparisons outlined in the MRA from theory to practice has not always been smooth or obvious. Different groups of metrologists working in different areas have interpreted the MRA in different ways. The practicalities of collecting data that support a specific measurement goal from laboratories all over the world has also had varying impact on the decisions made by the scientists who have planned and participated in Key Comparisons. Now, supported by a rich set of real comparisons from the KCDB and ICDB, an opportunity to study methods actually being used to conduct Key Comparisons has now arisen. This paper summarizes work on currently completed Key Comparisons and offers recommendations for the design, analysis, and interpretation of future comparisons.

Hornikova, A., Guthrie, W.F.	A Survey of Key Comparisons	Proceedings of the Measurement Science Conference 2005, Anaheim, California, January 2005	

Key Comparisons are international inter-laboratory studies used to establish the degree of equivalence between national measurement standards. These studies, carried out by National Metrology Institutes, are time-consuming, but necessary to facilitate international trade. Since the signing of the Mutual Recognition Arrangement (MRA) in 1999, approximately 120 Key Comparisons in a wide range of metrological areas have been completed and have results posted in the Key Comparison Database (KCDB) maintained by the International Bureau of Weights and Measures (BIPM) in France and in the International Comparisons Database (ICDB) maintained by the National Institute of Standards and Technology (NIST) in the U.S. As with many new standardized procedures, however, the translation of the guidelines for the conduct of Key Comparisons outlined in the MRA from theory to practice has not always been smooth or obvious. Different groups of metrologists working in different areas have interpreted the MRA in different ways. The practicalities of collecting data that support a specific measurement goal from laboratories all over the world has also had varying impact on the decisions made by the scientists who have planned and participated in Key Comparisons. Now, supported by a large set of completed comparisons from the KCDB and ICDB, an opportunity to study methods actually being used to conduct Key Comparisons has now arisen. This paper summarizes work on currently completed Key Comparisons and offers recommendations for the design, analysis, and interpretation of future comparisons.

Author	Title	Place of Publication	Date
Huang, I-F., Hwang, I-S., Shie, H-J.	Guaranteed Quality of Recovery in WDM Mesh Networks	IEEE Proceedings Communications Research Publication, 2005	

This study proposes a mechanism of guaranteed quality of recovery (GQoR) for Wavelength Division Multiplexing (WDM) mesh networks. Four GQoR levels are used to support customized services, and each of them is mapped to the adaptive recovery methodology. Once a failure occurs, the control system activates the recovery mechanism in compliance with the GQoR level. If the protection procedure fails as well, the proposed algorithm will then execute the restoration mechanism. Consequently, the recovery success rate is increased. This paper examines the shared segment recovery methods to establish backup path; therefore, it is well suited for large-scale networks and also increases the bandwidth utilization of the networks. Furthermore, a node deals only with its own routing information by employing the distributed control, so the fault recovery procedure can be speeded up. Simulation results reveal that the proposed method has greater performance of lower blocking probability and mean hop number than other methods previously reported in the literature.

Irvine, J.M., Fenimore, C.P., Cannon, D., Roberts, J., Israel, S.A., Simon, L., Watts, C., Miller, J.D., Avilés, A.I., Tighe, P.F., Behrens, R.J.	Feasibility Study for the Development of a Motion Imagery Quality Metric	Proceedings of Applied Imagery Pattern Recognition Workshop 2004, Washington, D.C., October 13-15, 2004	10/13/2004

The motion imagery community would benefit from the availability of standard measures for assessing image interpretability. The National Imagery Interpretability Rating Scale (NIIRS) has served as a community standard for still imagery, but no comparable scale exists for motion imagery. Several considerations unique to motion imagery indicate that the standard methodology employed in the past for NIIRS development may not be applicable or, at a minimum, require modifications. Traditional methods for NIIRS development rely on a close linkage between perceived image quality, as captured by specific image interpretation tasks, and the sensor parameters associated with image acquisition. The dynamic nature of motion imagery suggests that this type of linkage may not exist or may be modulated by other factors. An initial study was conducted to understand the effects of specific factors on perceived image interpretability for motion imagery. These factors are: Target motion: Other studies indicate that moving targets exhibit greater salience that can enhance target detection and recognition; Camera motion: The parallax effect and changing viewing geometry assist the analyst, particularly when viewing partially occluded targets; Scene complexity: It has been hypothesized that both target and camera motion exhibit greater effects on perceived interpretability when the scenes are more complex. In this evaluation, a number of experienced imagery analysts provided ratings and comparisons of a number of motion imagery clips and images derived from these clips. The image set was well characterized in terms of target motion, camera motion, and scene complexity, as well as ground sampled distance. Analysis of the data from this evaluation provides insight into the magnitude of these effects on perceived image interpretability. This paper describes the evaluation, presents the results, and explores the implications for development of a "NIIRS-like" scale for motion imagery.

Author	Title	Place of Publication	Date
Jansen, W., Ayers, R.	Guidelines on PDA Forensics, Recommendations of the National Institute of Standards and Technology	NIST SP 800-72, http://csrc.nist.gov/publications	11/15/2004

Forensic specialists periodically encounter unusual devices and new technologies normally not envisaged as having immediate relevance from a digital forensics perspective. The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with Personal Digital Assistants (PDAs), and to prepare forensic specialists to deal with new situations when they are encountered. This guide provides an in-depth look into PDAs and explains associated technologies and their impact on the procedures for forensic specialists. It covers the characteristics of three families of devices: Pocket PC, Palm OS, and Linux based PDAs and the relevance of various operating systems associated.

Kacker, R.N., Datla, R.U., Parr, A.C.	Response to Comments by Franco Pavese on Kacker et al., Metrologia 41 (2004) 340-352	Metrologia	

This is response to comments on our published papers submitted by Dr. Franco Pavese of the NMI of Italy.

Knill, E.H.	Quantum Computing with Very Noisy Devices	Nature and http://arxiv.org/quant-ph	10/19/2004

There are quantum algorithms that can efficiently simulate quantum physics, factor large numbers and estimate integrals. As a result, quantum computers can solve otherwise intractable computational problems. One of the main problems of experimental quantum computing is to preserve fragile quantum states in the presence of errors. It is known that if the needed elementary operations (gates) can be implemented with error probabilities below a threshold, then it is possible to efficiently quantum compute arbitrarily accurately. Here we give evidence that for independent errors, the theoretical threshold is well above 3% a significant improvement over earlier calculations. However, the resources required at such high error probabilities are excessive. Fortunately, they decrease rapidly with decreasing error probabilities. If we had quantum resources comparable to the considerable resources available in today's digital computers, we could implement non-trivial quantum algorithms at error probabilities as high as 1% per gate.

Author	Title	Place of Publication	Date
Kuhn, D.R., Walsh, T.J., Fries, S.	Security Considerations for Voice Over IP Systems, Recommendations of the National Institute of Standards and Technology	NIST SP 800-58, http://csrc.nist.gov/publications	1/5/2005

Voice over Internet Protocol (VOIP) refers to the transmission of speech across data-style networks. This form of transmission is conceptually superior to conventional circuit switched communication in many ways. However, a plethora of security issues are associated with still-evolving VOIP technology. This publication introduces VOIP, its security challenges, and potential countermeasures for VOIP vulnerabilities.

Leigh, S.D.	Book Review of Statistics for the Quality Control Chemistry Laboratory, by Eamonn Mullins	Analytical and Bioanalytical Chemistry	

Book Review

Lennon, E.B., Editor	2004 Information Technology Laboratory (ITL) Technical Accomplishments	NISTIR 7169	

This report presents the achievements and highlights of NIST's Information Technology Laboratory during FY 2004. Following the Director's Foreword and the ITL overview, the report describes technical projects in ITL research areas, followed by cross-cutting focus areas, industry and international interactions, publications, conferences, and staff recognition.

Lyon, G.E., Mink, A., Van Dyck, R.E.	Toward an Architectural Framework to Improve Accountability in the Use of Electronic Records	NISTIR 7157	

Sensitive electronic record systems (ERSs) raise questions about their proper use. Insider-threat involves hidden, unknown and unanticipated activities that constitute unacceptable use of an ERS, even while operating within individual access privileges. Insider-threat detection and control is an ERS monitoring and management challenge of the first order. A flexible preliminary framework can encourage discussion and comparison among various monitoring elements for the insider-threat. Responding to a lack of such a framework, one is sketched here: It employs two perspectives of an ERS user -- structural and intentional. The structural view is short term, whereas the intentional view seeks to discover general content topics of interest to a user, and to follow these over time. Discussion includes details of a possible architecture that uses untrained classification methods to amplify the concern set beyond that specifically defined at the onset of monitoring. The general framework may expedite development of common guidelines and methodologies to monitor insider threats. Although developed for medical services (e.g., an E-Health RS), the framework likely has applicability in other similar database areas such as security and intelligence archiving.

Author	Title	Place of Publication	Date
Micheals, R.J., Boult, T.E.	Is the Urn Well-Mixed? Uncovering False Cofactor Homogeneity Assumption in Evaluation	NISTIR 7156	10/27/2004

Measuring system performance is conceptually straightforward; it is the interpretation of the results and their use as predictors of future performance that are the exceptional challenges in system evaluation and the experimentation in general. Good experimental design is critical in evaluation, but there have been very few techniques that a scientist may use to check their design for either overlooked associations or weak assumptions. For biometric and vision system evaluation, the complexity of the systems make a thorough exploration of the problem space impossible. This lack of verifiability in experimental design is a serious issue. In this paper, we present a new evaluation methodology that aids the researcher in discovering false assumptions about the homogeneity of cofactors – when the data is not “well mixed.” The new methodology is then applied in the context of a biometric system evaluation.

Mills, K., Tan, C.	Performance Characterization of Decentralized Algorithms for Replica Selection in Distributed Object Systems	TBD	

Designers of distributed software systems often rely on server replicas for increased robustness, scalability, and performance. Replicated server architectures require some technique to select a target replica for each client transaction. In this paper, we survey key concepts related to replica selection and we use simulation to characterize performance (response time, server latency, selection error, probability of server overload) for four common replica-selection algorithms (random, greedy, partitioned, weighted) when applied in a decentralized form to client queries in a distributed object system deployed on a local network. We introduce two new replica-selection algorithms (balanced and balanced-partitioned) that give improved performance over the more common algorithms. We find the weighted algorithm performs best among the common algorithms and the balanced algorithm performs best among all those we considered. Our findings should help designers of distributed object systems to make informed decisions when choosing among available replica-selection algorithms.

Author	Title	Place of Publication	Date
Oelbaum, T., Baroncini, V., Tan, T.K., Fenimore, C.	Subjective Quality Assessment of the Emerging AVC/H.264 Video Coding Standard	Proceedings of the International Broadcast Symposium 2004, Amsterdam, Netherlands, September 9–13, 2004	

The results of a formal subjective test comparing the AVC/H.264 video coding standard with the widely used MPEG-2 video coding standard was recently released by the MPEG working group. New products based on the recently completed AVC/H.264 video coding standard are being announced every other week. Similarly, there have been numerous reports and claims about the visual quality that can be achieved with this new standard. It is therefore important for the broadcasting community to understand the actual benefits that come with this new video coding standard compared to previous standards. This paper tries to give further insights and indications to the important question on what the benefits and gains really are. An introduction to the above test and a description of the test conditions and the test environment evaluation is presented. This is followed by results from subjective tests of current standard television resolution as well as ATV up to HDTV resolutions. This work is the result of the activities of the JVT/MPEG Ad Hoc Group on AVC Verification Test. The authors of this paper acted as chairmen of the Ad Hoc Group during the period it was active from July 2002 to December 2003.

Phillips, P.J., Flynn, P.J., Scruggs, T., Bowyer, K.W., Chang, J., Hofman, K., Marques, J., Min, J., Worek, W.	Overview of the Face Recognition Grand Challenge	NISTIR 7195 and IEEE Computer Society International Conference on Computer Vision and Pattern Recognition 2005	

Over the last couple of years, face recognition researchers have been developing new techniques, such as recognition from three-dimensional and high resolution imagery. These developments are being fueled by advances in computer vision techniques, computer design, sensor design, and interest in fielding face recognition systems. These techniques hold the promise of reducing the error rate in face recognition systems by an order of magnitude over FRVT 2002 results. The Face Recognition Grand Challenge (FRGC) is designed to achieve this performance goal by making available to researchers a data corpus of 50,000 images and a challenge problem containing six experiments. The data consists of 3D scans and high resolution still imagery. The imagery is taken under controlled and uncontrolled conditions. This paper describes the data corpus and challenge problems, and presents baseline performance and preliminary results on natural statistics of facial imagery.

Author	Title	Place of Publication	Date
Podio, F.L.	International Biometric Standards - Addressing the Customer Needs for Personal Authentication	ISO Focus (Magazine of the International Organization for Standardization)	

Authentication is the provision of assurance of the claimed identity of an entity. Biometrics is defined as the automated recognition of individuals based on their behavioral and biological characteristics. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. Biological characteristics include hand and facial features, fingerprints, and iris patterns. In addition to supporting national security and preventing ID fraud, they are starting to play a crucial role in enterprise-wide network security infrastructures, the protection of buildings from unauthorized individuals, employee IDs, secure electronic banking and financial transactions, retail sales, law enforcement and health and social services. Mobile devices, colleges, and amusement parks are already benefiting from these technologies. In the last few years, national security priorities have emphasized the need for biometrics in employee identification documents, passports and other high secure applications. These activities are inherently global in scope. These needs for biometric technologies have encouraged international biometric standardization. ISO/IEC JTC 1 established Subcommittee 37 – Biometrics in June 2002 in response to these users' immediate needs, and to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of biometric standards. Twenty seven member countries are involved in this endeavor. The article describes the current activities of this Subcommittee, its program of work, and the interrelationship with other standards bodies and outside organizations. It emphasizes also early adoption of international biometric standards developed under SC 37 by large organizations such as the International Civil Aviation Organization and the International Labor Organization of the UN.

Quirolgico, S., Assis, P., Westerinen, A., Baskey, M., Stokes, E.	Toward a Formal Common Information Model Ontology	Ontologies for Networked Systems (ONS04)	

Self-managing systems will be highly dependent upon information acquired from disparate applications, devices, components, and subsystems. To be effectively managed, such information will need to conform to a common model. One standard that provides a common model for describing disparate computer and network information is the Common Information Model (CIM). Although CIM defines the models necessary for inferring properties about distributed systems, its specification as a semi-formal ontology limits its ability to support some important requirements of a self-managing distributed system including knowledge interoperability and aggregation, as well as reasoning. To facilitate the interoperability and aggregation of CIM-based knowledge, as well reasoning over such knowledge, there is a need to model, represent, and share CIM as a formal ontology. In this paper, we propose a framework for constructing a formal CIM ontology based on previous research that identified mappings from UML to ontology language constructs.

Author	Title	Place of Publication	Date
Roginsky, A.L.	Targeted Search: Reducing the Time and Cost for Searching for Objects in Multi-Server Networks	24th IEEE International Performance, Computing, and Communications Conference, Phoenix, Arizona, April 7-9, 2005	

In many applications – including P2P file sharing, content distribution networks, and grid computing – a single object will be searched for in multiple servers. In this paper, we find the provably optimal search method for such applications and develop analytical models for search time and cost. A client node searching for objects maintains statistics on where (in which servers) it has previously found objects. Using these statistics to target future searches to “popular” servers is provably optimal. For object location and request distributions that are non-uniform, which has been shown to be the case in P2P file sharing networks, this method of targeted searching is found to be more cost-effective (i.e., use less server resources) than broadcast-based searching. Our targeted search method is implemented in a prototype Gnutella servent called Ditella. Ditella can improve the scalability of file sharing in P2P networks and reduce the amount of traffic in the Internet by reducing file search query traffic.

Ross, R.S., Toth, P.R.	Understanding the NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government	ITL Bulletin, November 2004	11/29/2004

This ITL Bulletin summarizes an article entitled "Understanding the New FISMA Required NIST Standards and Guidelines,” by Ron S. Ross, PhD.

Rouil, R., Chevrollier, N., Golmie, N.	Unsupervised Anomaly Detection System Using Next-Generation Router Architecture	TBD	

Unlike many intrusion detection systems that rely mostly on labeled training data, we propose a novel technique for anomaly detection based on unsupervised learning and we apply it to counter denial-of-service attacks. Initial simulation results suggest that significant improvements can be obtained. We then discuss an implementation of our anomaly detection system in the ForCES router architecture and evaluate it using attack traffic.

Author	Title	Place of Publication	Date
Scholtz, J.C.	The Effect of Situation Awareness Acquisition in Determining the Ratio of Operators to Semi-Autonomous Driving Vehicles	The International Society for Optical Engineering	

We used a technical readiness level assessment to obtain intervention time and the time to acquire situation awareness for different classifications of interventions. We analyzed this data to determine if it is feasible for one operator to control multiple robots of this type in similar environments. We conclude that in both terrains analyzed (an arid terrain and a wooded terrain) it would be feasible for one operator to control two robots. While it is also possible for an operator to work on another task and control a robot as well, there is an issue of providing situation awareness about the robot. There are also constraints on the tasks that could be effectively accomplished.

Scholtz, J.C., Antonishek, B., Young, J.D.	Evaluation of Human-Robot Interaction in the NIST Reference Search and Rescue Test Arenas	Performance Metrics for Intelligent Systems 2004 Workshop Proceedings, PerMIS '04	

We describe data collections that we have conducted during Urban Search and Rescue (USAR) competitions within the NIST Reference Test Arenas. We also discuss our analyses of this data and present guidelines based on these studies. We also describe future plans for augmenting USAR competitions to specifically compare different methods of human-robot interaction (HRI).

Slattery, O.T.	Drive Compatibility Test (Phase 2) for DVD-R (General) and DVD+R Discs, Including DVD Creation Plan	NIST SP 500-258	10/19/2004

Phase 2 test procedure is designed to test the compatibility of DVD drives with DVD writable media including DVD-R (for general) and DVD+R. The test plan includes detailed instructions on how to create and test the recordable media and how to determine the result from each test. Following implementation of Phase 1 (NIST Special Publication 500-254), the National Institute of Standards and Technology (NIST), the Optical Technology Storage Association (OSTA) and the DVD Association (DVDA) expanded the scope of testing in Phase 2. Phase 2 includes testing of DVD recordable drives and also includes a procedure to create test media.

Author	Title	Place of Publication	Date
Somma, R., Barnum, H., Knill, E.H., Ortiz, G., Viola, L.	Generalized Entanglement and Quantum Phase Transitions	International Journal of Modern Physics B	

Quantum phase transitions in matter are characterized by structural changes in some correlation functions of the system, thus ultimately entanglement. In this work, we study the second order quantum phase transitions present in models of relevance to condensed-matter physics by exploiting the notion of generalized entanglement [Barnum et al., Phys. Rev. A 68, 032308 (2003)]. In particular, we focus on the illustrative case of a one-dimensional Ising model in the presence of a transverse magnetic field. Our approach leads to useful tools for distinguishing between the ordered and disordered phases in the case of broken symmetry quantum phase transitions. Possible extensions to the study of other kinds of phase transitions as well as of the inherent relation between generalized entanglement and computational efficiency are also discussed.

Souryal, M.R., Larsson, E.G., Peric, B.M., Vojcic, B.R.	Soft Decision Metrics for Turbo-Coded FH M-FSK Ad Hoc Packet Radio Networks	2005 IEEE Vehicular Technology Conference (VTC 2005/Spring)	

This paper addresses turbo-coded non-coherent FH M-FSK ad hoc networks with a Poisson distribution of interferers where multiple access interference can be modeled as symmetric a-stable (SaS) noise and a is inversely proportional to the path loss exponent. The Bayesian Gaussian metric does not perform well in non-Gaussian (a?2) noise environments and therefore an optimum metric for Cauchy (a=1) noise and a generalized likelihood ratio (GLR) Gaussian metric requiring less side information (amplitude, dispersion) are presented. The robustness of the metrics is evaluated in different SaS noise environments and for mismatched values of the interference dispersion and channel amplitude in an interference-dominated network with no fading or independent Rayleigh fading. Both the Cauchy and GLR Gaussian metric exhibit significant performance gain over the Bayesian Gaussian metric, while the GLR Gaussian metric does so without the knowledge of the dispersion or amplitude. The Cauchy metric is more sensitive to the knowledge of the amplitude than the dispersion, but generally maintains better performance than the GLR Gaussian metric for a wide range of mismatched values of these parameters. Additionally, in an environment consisting of non-negligible Gaussian thermal noise along with multiple access interference, increasing the thermal noise level degrades the performance of the GLR Gaussian and Cauchy metric while for the observed levels both maintain better performance than the Bayesian Gaussian metric.

Souryal, M.R., Larsson, E.G., Peric, B.P., Vojcic, B.R.	Soft-Decision Metrics for Coded Orthogonal Signaling in Symmetric Alpha-Stable Noise	Proceedings of the 2005 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)	

This paper derives new soft decision metrics for coded orthogonal signaling in symmetric a-stable noise, which has been used to model impulsive noise. In addition to the optimum metrics for Gaussian (a = 2) noise and Cauchy (a = 1) noise, a class of generalized likelihood ratio (GLR) metrics with lower side information requirements is derived. Through numerical results for a turbo code example, the Cauchy decoder is found to be robust for a wide range of a, and GLR metrics are found which provide performance gains relative to the Gaussian metric, but with lower complexity and less a priori information.

Author	Title	Place of Publication	Date
Stanford, V., Rochet, C., Michel, M., Garofolo, J.	Beyond Close Talk - Issues in Distant Speech Acquisition, Conditioning Classification, and Recognition	Included in NIST SP 500-257, Proceedings of the ICASSP 2004 Meeting Recognition Workshop, http://www.itl.nist.gov/iad/IADpapers/2004/ICASSP2004Workshop.pdf	10/14/2004

Properly designed reference data and performance metrics can offer crucial aid to developers of advanced statistical recognition technologies. We focus here on audio data acquisition from close-talk, nearfield, and farfield sensors, and upon its processing, and its metrology. Our intention is to support the research community as it develops state of the art data acquisition and multimodal processing algorithms by supplying standard reference data, metrics, and sharable infrastructure.

Theofanos, M.F., Scholtz, J.	A Diner's Guide to Evaluating a Framework for Ubiquitous Computing Applications	Human Computer Interface International Conference 2005	

There is a clear need for evaluation methodologies specifically suited to ubiquitous computing applications. Here we investigate a user evaluation framework we proposed earlier which draws upon traditional desktop methods, but carefully adapts them based on our experiences with ubiquitous architectures. We test and clarify the criteria in our methodology by examining the utility and applicability of the framework to an existing commercial ubiquitous application for restaurant ordering at the tableside. We analyzed its functionality by discussing design principles with its software developers, and interviewed wait staff as well as restaurant managers to understand its impacts on the workflow and business processes. We conclude that the proposed framework does contain appropriate metrics to assess whether good design principles were achieved and if the designed system will produce the desired user experience.

Toman, B.	Linear Statistical Models With Type B Uncertainty: A Bayesian View of Annex H.3 and H.5 of the Guide to the Expression of Uncertainty in Measurement	Metrologia	

Annex H.3 of the Guide to the Expression of Uncertainty in Measurement presents an example of calibration of a thermometer using a linear regression model. Annex H.5 of the same publication presents a class of statistical models and analysis techniques which are commonly called the Analysis of Variance (ANOVA). These models are useful for accounting for the effects of factors which cause the measurand in an experiment to change over time or over experimental conditions. Both Annex H.3 and H.5 present procedures which assume that the observations are not subject to type B uncertainties. A natural question then is: Can these models be used in the presence of type B uncertainties? This article answers the question in the affirmative and provides a natural interpretation of the results. The example data from the two Annexes are used for an illustration.

Author	Title	Place of Publication	Date
Walsh, T.J., Kuhn, D.R.	Securing Voice Over Internet Protocol Networks	ITL Bulletin, October 2004	10/28/2004

Voice over IP – the transmission of voice over traditional packet-switched IP networks – is one of the hottest trends in telecommunications. As with any new technology, VOIP introduces both opportunities and problems. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but security administrators will face significant challenges. Administrators may assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks. Unfortunately, many of the tools used to safeguard today's computer networks, namely firewalls, Network Address Translation (NAT), and encryption, carry a hefty price when incorporated into a VOIP network. This paper introduces the security issues with VOIP and outlines steps that can be taken to operate a VOIP system securely.

Wang, C.M., Iyer, H.K.	Detection of Influential Observation in the Determination of the Weighted-Mean KCRV	Metrologia	

Since the signing of the Mutual Recognition Arrangement, National Metrology Institutes (NMI) have carried out many key comparisons in a wide range of metrological areas to establish the equivalence of their measurement standards. The determination of a key comparison reference value (KCRV) and its associated uncertainty are the central tasks in the evaluation of key comparison data. One of the most popular ways to estimate the KCRV is to use a weighted mean of each NMI's reporting values, with weights inversely proportional to the variances of the NMI's reporting value. One potential problem with the use of the weighted mean is its reliance on the weights that may vary greatly across NMIs. Consequently, some of the NMIs can be influential in the determination of the weighted-mean KCRV. Thus it is of interest to identify the influential NMIs based on some simple and well-defined criteria. In this paper, we present several easy-to-use criteria for detecting influential data in the calculation of the weighted-mean KCRV.

Author	Title	Place of Publication	Date
Wang, Q., Ressler, S.	A Tool Kit to Generate 3D Animated CAESAR Bodies	2005 SAE Digital Human Modeling For Design and Engineering Symposium, Iowa City, Iowa, June 14-16, 2005	

The Civilian American and European Surface Anthropometry Resource (CAESAR) database provides a comprehensive source for body measurement in numerous industries such as apparel, aerospace, and automobile. Generating animated CAESAR body sequences from still surface and landmark data will stimulate research and design in these areas. A tool kit has been developed to convert CAESAR bodies to models compliant with the Humanoid Animation specification (H-Anim). It will be helpful to set up a realistic motion capable humanoid library for application environment that can be reused in a wide variety of ergonomic applications. The process consists of preprocessing the mesh, building a skeleton structure, creating segments of the body, assigning weights for vertices, and integrating motion capture data. Publicly available software is adopted for mesh compression and hole filling. C programs were developed to implement the translation from CAESAR body data to H-Anim. The technical issues involved in the process are discussed, and experimental results are shown in the paper.

Wang, Q., Saunders, B.	Web-Based 3D Visualization in a Digital Library of Mathematical Functions	NISTIR 7159 and Conference Proceedings of the WEB3D 2005 Symposium, University of Wales, United Kingdom, March 29–April 1, 2005	12/1/2004

The National Institute of Standards and Technology (NIST) is developing a digital library of mathematical functions to replace the widely used National Bureau of Standards Handbook of Mathematical Functions published in 1964 [1]. The NIST Digital Library of Mathematical Functions (DLMF) will provide a wide range of information about high-level functions for scientific, technical and educational users in the mathematical and physical sciences. Clear, concise 3D visualizations that allow users to examine poles, zeros, branch cuts and other key features of complicated functions will be an integral part of the DLMF. Specially designed controls will enable users to move a cutting plane through the function surface, select the surface color mapping, choose the axis style, or transform the surface plot into a density plot. To date, Virtual Reality Modeling Language and Extensible 3D (VRML/X3D) standards have been used to implement these capabilities in more than one hundred 3D visualizations for the DLMF. We discuss the development of these visualizations, focusing on the design and implementation of the VRML code, and show several examples.

Author	Title	Place of Publication	Date
White, D., Tebbutt, J.	A Perl-Based Framework For Distributed Processing	Open Source Developers' Conference 2004, Melbourne, Australia, December 1-3, 2004	

The National Software Reference Library (NSRL) of the U.S. National Institute of Standards and Technology (NIST) collects software from various sources and publishes file profiles computed from this software (such as MD5 and SHA-1 hashes) as a Reference Data Set (RDS) of information. The RDS can be used in the forensic examination of file systems, for example, to speed the process of identifying unknown or suspicious files. This paper describes the cross-platform, public domain, Linux/Apache/MySQL/Perl (LAMP) framework with which we produce the RDS from acquired software. The framework is easily deployed (it has been packaged on a Knoppix-based live CD) and allows for the distributed processing of large numbers of files in a loose, heterogeneous computing cluster. We go on to suggest that the framework is sufficiently general in its implementation to be suitable for application to classes of problems quite beyond our original scope.

Wu, J.C., Wilson, C.L.	Nonparametric Analysis of Fingerprint Data	NISTIR 7168	

This paper demonstrates that, for large-scale tests, the match and non-match similarity scores have no specific underlying distribution function. The forms of these distribution functions require a nonparametric approach for the analysis of the fingerprint similarity scores. In this paper, we present an analysis of the discrete distribution functions of the match and non-match similarity scores of the fingerprint data that clarifies the widely varying form of these distribution functions. This analysis demonstrates that a precise Receiver Operating Characteristic (ROC) curve based on the True Accept Rate (TAR) of the match similarity scores and the False Accept Rate (FAR) of the non-match similarity scores can be constructed without any assumption regarding operating thresholds or the form of the distribution functions. The area under such a ROC curve, assuming normality, is equivalent to the Mann-Whitney statistic directly formed from the match and non-match similarity scores. In addition, the Z statistic computed using the areas under ROC curves along with their variances is applied to test the significance of the difference between two ROC curves. Four examples than from NIST's extensive testing of commercial fingerprint systems are provided. The nonparametric approach presented in this article can also be employed in the analysis of other biometric data.

Yanik, L., Torre, E.D., Donahue, M.J., Cardelli, E.	Micromagnetic Eddy Currents in Conducting Cylinders	Journal of Applied Physics	

The inclusion of eddy currents into micromagnetic programs is important for the proper analysis of dynamic effects in conducting magnetic media. This paper introduces a limited numerical implementation for eddy current calculations and discusses some interesting analytic cases in the simplified geometry. It is designed to provide some benchmarks for more complex program.

Author	Title	Place of Publication	Date
Zhang, N.F.	Statistical Process Control in Biochemical and Hematological Quality Control Data	Proceedings of the American Statistical Association	

Daily quality control (QC) measurements of common biochemical and hematological quantities were recorded during several months while methods and analyzers showed no signs of malfunctioning. Usually it is assumed that QC data may be described as i.i.d. In this case an X chart and/or an EWMA chart are the proper control charts to use. When autocorrelation is presented, the traditional control charts may be inefficient. An alternative control chart, the EWMAST chart proposed in Zhang (1998) has been developed for stationary process data. The EWMA and the EWMAST chart were applied to each of the 11 QC data series. In 6 of the 11 series, significant process autocorrelations were demonstrated. The results show that the conventional EWMA chart may give false alarms in the presence of autocorrelation while the EWMAST chart gave few false alarms.

Zhang, N.F., Winkel, P.	The Effect of Recalibration and Reagent Lot Changes on the Performance of QC Control Charts	Clinical Chemistry	

Daily QC measurements of biochemical quantities were recorded during four to five months while methods and analyser showed no signs of malfunctioning. The time series of QC values were divided into subseries according to reagents or electrolyte diluent lot and (within diluent subseries) disposable electrode used. ANOVA was used to examine if the mean level changed significantly between subseries. All time series, as well as reagents and diluent subseries were examined for autocorrelation. The X-chart and the EWMAST (in autocorrelated series) or EWMA chart were applied to each time series and each reagents and diluent subseries and the number of values falling outside the 3 SD control limits were noted. Results: The mean levels changed significantly due to diluent lot changes, replacement of disposable electrodes and recalibrations following reagents lot changes. These changes caused spurious autocorrelation as evidenced by the ACF plot. In 42% of all reagents subseries a significant autocorrelation could also be demonstrated; however, 5.64% and 29.1% of all time series values fell outside the control limits of the X-charts and the EWMA or EWMAST charts respectively. These percentages were reduced to 0.44 and 0.7 when separate control charts were calculated following recalibrations and changes of diluent lot. Conclusions: The mean level may change due to recalibrations and change of electrode diluent lot that causes an excessive number of false alarms unless new control charts are calculated subsequent to these events.

Author	Title	Place of Publication	Date
Ziring, N., Wack, J.	Specification for the Extensible Configuration Checklists Definition Format (XCCDF)	NISTIR 7188	

This document specifies the data model and XML representation for the Extensible Configuration Checklist Description Format. An XCCDF document is a structured collection of security configuration rules for some set of target systems. The XCCDF specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.